2026年度西安市水务局信息化系统运维项目（新增运维）

采购内容及要求

一、项目维护服务的内容、预期目标：

1.1 项目概况

西安市地处关中平原腹地，南依秦岭，北临渭河，地理位置特殊，防汛形势复杂严峻。秦岭山区降雨丰富，山洪灾害监测预警任务艰巨；作为特大城市，城市内涝防御压力巨大。全市现有水利工程数量众多，监测点位分散，流域面积广，传统的人工巡查方式无法满足现代防汛工作的时效性和准确性要求。面对日益复杂的气候变化和极端天气事件频发的严峻形势，西安市水务局深刻认识到，必须依靠信息化手段，构建现代化的智慧水务与防汛管理体系，才能有效提升水灾害防御能力和水务治理现代化水平。

近年来，在市委、市政府的正确领导下，西安市水务局大力推进水务信息化建设，新增智慧水务平台、水库大坝监测与运行管理系统、水灾害防御平台等重点水务信息化系统，业务范围涵盖智慧水务、智慧防汛、城市内涝、水库监测、防汛物资管理等关键领域，是保障城市水安全、优化水务管理效能、防范水灾害风险的重要基础，所有项目均已通过竣工验收并处于正常运行状态。

1.2 运维必要性

目前，智慧水务平台为全市水务领域提供重要数据支撑，是全市水务领域重要数据交换共享中枢，承担着统一门户访问登录，数据统一汇集，安全一体化防护等重要环节。新增模块运维包括智慧水务总平台及水库大坝、智慧防汛内涝、物资库管理3个业务模块，这些模块已在西安市防汛减灾和水务管理工作中发挥了重要作用，成为全市开展水旱灾害防御、城市排水防涝、水库安全调度、水资源配置等工作的综合性支撑平台。在防汛减灾方面，系统通过全天候监测、智能预警预报、一体化应急响应，显著提升了山洪灾害预警、城市内涝防御、水库安全监测能力，为防汛指挥决策提供了重要的技术支撑，在防汛工作过程中，能够提前研判、科学调度，最大程度减轻了水灾害造成的损失，有效守护了人民生命财产安全。在水务管理方面，系统整合了水文、水质、气象、生态等全维度水务信息资源，打破了数据孤岛，构建了统一的数据资源中心和应用服务平台，实现水务管理从经验型向数据型、从分散型向协同型、从被动响应向主动应对的转变，全面提升了水务管理精细化、智能化水平。

这些信息化系统的持续稳定运行，离不开专业、规范、高效的运行维护工作。首先，防汛工作事关人民群众生命财产安全，系统必须安全稳定运行，任何一个环节的故障都可能导致监测数据的缺失或预警信息的延迟，造成无法估量的损失，因此必须通过专业运维确保系统的稳定性和可靠性。其次，防汛系统的数据准确性直接关系到决策的科学性，硬件设备在野外恶劣环境下长期运行必然会出现老化、损坏等问题，必须通过定期巡检、及时更换维护、校准标定等措施，确保监测数据的准确性和一致性，为决策提供可靠支撑。第三，防汛工作时效性极强，系统故障必须在最短时间内得到排除，需要建立专业化的技术团队，确保故障发现及时、响应迅速、处置有效。因此，建立健全运维管理体系，落实专项运维经费，开展常态化专业化运维服务十分必要。

1.3 运维目标

随着水务数字化转型加速，原有分散式运维模式面临效率低、成本高等问题。为进一步做好运维管理，2025 年成立了西安市水务信息宣传教育中心，负责统筹全局信息化系统运维工作。

本次运行维护项目核心目标是建立一个高效可靠的运维体系，保证全部运维对象处于高效稳定的运行状态，通过信息化手段为防汛指挥决策提供技术支撑，最大程度减少水灾害造成的损失，守护人民生命财产安全。具体运行维护目标可概括如下：

（1）稳定性保障：通过常态化监控与预防性维护，保障运维对象稳定平稳运行。

（2）性能优化：持续优化架构与配置，提升运维对象运行性能。

（3）故障快速响应：建立高效故障处理机制，确保故障有效处置时间符合运行维护服务方案要求。

（4）安全合规：落实安全防护措施，按要求开展安全检测与漏洞修复，保障系统安全可靠。

（5）服务标准化：建立规范的运维流程与文档体系，确保运维操作可追溯、服务质量可量化，提升用户对运维服务的满意度。

1.4 项目运维对象基本情况

（一）信创、等保、密评情况

信创、等保、密评方面，本次申报的智慧防汛前端监测感知与系统应用开发集成运维模块、西安市水库大坝监测与运行管理系统模块、西安市水务局智慧水务平台运维模块均符合网络安全等级三级保护标准，已通过信息安全等级保护测评，已通过密码应用安全性评估。西安市水务局负责 2026 年等保、密评测评工作，统一纳入西安市大数据局集采范围。

项目严格遵守国家保密法律法规与测评要求，全程协同配合测评机构的审查与检测工作，主要完成政务网内运维客户端安全认证服务改造、应用系统统一安全认证服务对接改造、关键业务数据签名验签服务改造、对重要数据进行数据库加密存储、启用基于国密算法的 SSL 证书进行系统访问等。

信创适配方面，项目完全适配国产自主可控要求。

信创适配情况

序号	产品	使用信创产品情况
1	云服务器	操作系统：Huawei cloud EulerOS 2.0(aarch64) CPU：鲲鹏
2	数据库软件	数据库：人大金仓数据库，达梦数据库 V8，华为 GaussDB 8.0.28
3	中间件	中间件：东方通
4	浏览器	浏览器：奇安信浏览器
5	渲染服务器	CPU：海光 操作系统：银河麒麟桌面操作系统 V10（SP1）
6	模型计算服务器	CPU：鲲鹏 920 操作系统：银河麒麟 V10 服务端操作系统

（二）软件情况

2026 年度西安市水务局信息化系统新运维项目软件主要包括智慧防汛前端监测感知与系统应用开发

集成、西安市水库大坝安全监测和运行管理系统、西安市水务局智慧水务平台。软件均部署于西安市政务云上，智慧防汛前端监测感知与系统应用开发集成、西安市水库大坝安全监测和运行管理系统均通过单点登录方式挂载于西安市水务局智慧水务平台，通过智慧水务平台访问且独立运行。

（1）智慧防汛前端监测感知与系统应用开发集成

智慧防汛前端监测感知与系统应用开发集成运维模块建设了城市内涝淹没分析模型、防汛数字底座、水灾害防御平台扩展升级、智慧防汛平台，物资库管理。为确保软件运行维护、迭代升级等后续工作有序开展，发挥平台最大效益，经市水务局与市应急局协商一致，双方同意将智慧防汛平台软件成果及相关全部技术文档移交市应急局，市水务局负责做好该软件水务数据资源支撑保障，2027 年起由市应急局只负责申请智慧防汛平台的软件运维经费，市水务局只负责申请智慧防汛前端监测感知与系统应用开发集成建设内容的运维经费。另外，城市内涝分析功能属西安市水务局维护范围，该功能对全市防汛意义重大，西安市水务局通过该功能分析内涝淹没情况，为西安市委市政府、市应急局等其它市级部门提供防汛数据支撑。因此，该项工作需要不断率定、优化、提升，需要的工作量较大，周期较长，维护成本较高。西安市水务局负责维护的内容如下：

水灾害防御平台扩展升级基于市水务局水灾害防御平台，以城市内涝淹没分析模型为支撑，对接省级山洪灾害监测预警平台，扩展城市内涝防御、应急响应处置、预案智能驱动、措施保障等功能应用，打造防洪排涝一体化的水灾害防御系统，为智慧防汛平台提供数据和功能支撑。系统功能建设主要包括大屏端、山洪灾害、城市内涝、响应处置、措施保障（扩展）、系统管理（扩展）、APP 端（扩展）。

软件部署于西安市政务云西咸分节点（华为云）政务外网区。目前在免费运维期，由建设单位专人开展运行维护，目前软件运行状态正常。

城市内涝淹没分析模型主要包括支撑智慧防汛业务的核心软件模块、模型接口：

物理机理模型：包含城市产流水文模型（支持下渗、蒸腾计算）、一维管网/河道水动力模型、二维地表水动力模型及厂站网河联合调度模拟。

快速预报模型：基于机器学习算法开发的内涝过程及河道洪水快速预报模型（基于 3m 分辨率 DEM）。

数据对接服务：包含与气象局未来 60 小时降雨预报数据、物联监测实时数据（积水点、水位、流量）的自动化采集与预处理接口。

成果集成接口：负责将模型推演的积水深度、范围等计算成果实时推送到智慧防汛展示层。

（2）西安市水库大坝安全监测和运行管理系统

西安市水库监测设施项目根据前期方案在西安市大数据局、四个区县水务局分别部署“西安市水库大坝安全监测和运行管理系统采集服务器”用于接收和展示 49 个中小型水库的前端监测设备发来的数据，在发预警时能够及早通知相关的管理人员和单位。西安市水库大坝安全监测和运行管理系统采用分级分类的方式展现水库大坝监测数据，监督水库管理单位巡查工作安全。通过每天的信息汇总和管理人员的上报情况能够真实保留了历史数据，对于集中化掌控全市水库的安全状态提供了强有力的平台支撑。

软件主要包括平台软件、物联网接收平台、区县数据接收及解析软件，用户主要面向西安市水务局水库监督管理单位。

（3）西安市水务局智慧水务平台

智慧水务平台主要包括数据资源中心、应用支撑底座、统一门户、智慧水务一张图、“中央水塔” 专题应用，以及在涝峪安装三处土壤墒情站，目前系统正常运行中。该项目于 2025 年 12 月 9 日完成竣工验收，符合网络安全等级三级保护标准，通过信息安全等级保护测评，通过密码应用安全性评估，项目严格遵守国家保密法律法规与测评要求，全程协同配合测评机构的审查与检测工作，主要完成政务网内运维客户端安全认证服务改造、应用系统统一安全认证服务对接改造、关键业务数据签名验签服务改造、对重要数据进行数据库加密存储、启用基于国密算法的 SSL 证书进行系统访问等。信创适配方面，项目完全适配国产自主可控要求。

（二）硬件方面

硬件方面，本次申报运行维护的硬件设备主要包括 48 处城市积水点视频监控，36 处排口视频监控，35 处河道视频监控，水灾害防御库房 18 处监控、网络及相关硬件设备，5 台服务器（自建模型及渲染服务器，3 台部署于本地，2 台托管于凤八机房，都属于市水务局的维护内容）。在全市 49 座水库上，分别安装了边缘融合数据网关 52 台，监测站出口防火墙 11 台，视频监控站 26 处，万兆接入交换机 4 台，监测数据管理存储设施 8 台（部署于水库管理站），网络硬盘录像机 8 台，区县出口防火墙 4 台。（硬件设备清单详见附件一）

设备现状：硬件设备主要分布于偏远山区及城市管网，环境恶劣，但最早安装于 2022 年，建设单位一直认真负责建设期间的设备维护及保养工作。西安市水务局 2026 年 3 月 10 日启动了汛前维护工作。已完成全部硬件设备检查，校准雨量、水位信息 12 站次，维护胶体蓄电池 2 组，更换 3 台太阳能充电控制器，修剪 4 处站点遮挡树枝，更换 12 台路由器。目前所有设备运行状态良好，硬件设备在线率≥95%。

设备在线率统计表

序号	设备名称	设备数量	在线率
1	视频监控	163	96%
2	服务器	5	100%
3	边缘融合数据网关	52	100%
4	监测站出口防火墙	11	100%
5	万兆接入交换机	4	100%
6	监测数据管理存储设施	8	100%
7	网络硬盘录像机	8	100%
8	区县出口防火墙	4	100%

本次西安市水库大坝安全监测和运行管理系统涉及 49 座水库，多数分布于距市中心 30 至 100 公里，与城区维护点位相比，地理位置偏远，维护难度显著增加。具体表现为：单次维护作业路程往返时间长、人力资源投入大、人力成本高。

二、运维服务主要内容：

采购包 1（智慧水务及水库监测模块）：

2.1 运维方案设计

一、运维管理制度

运维团队需建立明确的运维管理制度，涵盖软件运维、硬件运维、安全运维等方面，明确工作流程、工作标准、工作产出物，实现运维工作的标准化、规范化、精细化，为系统安全稳定运行提供坚实保障。

二、运维组织架构

组建专业运行维护团队，具体组织架构如下图：



三、运维人员配置

运维团队人员配置如下：

序号	类型	岗位	人数
1	运维项目经理	项目经理	1
2	技术保障组	系统软件工程师	2
3		数据库工程师	2
4		硬件工程师	2
5	运行保障组	软件运维工程师	3
6		硬件运维工程师	3
7	安全保障组	安全工程师	2

四、运维岗位职责

运维团队岗位职责如下：

序号	岗位	核心职责
1	项目经理	统筹运维服务工作，制定服务计划，协调资源解决重大故障，对接用户需求并同步服务进展，负责服务质量评估与优化。
2	系统软件工程师	负责应用系统的运行监控、故障排查、版本更新与用户支持。
3	数据库工程师	负责数据运维工作，包括性能优化、备份恢复、索引管理与故障处理等。
4	硬件工程师	负责前端硬件设备的故障处理、设备修复、固件升级等工作。
5	软件运维工程师	负责现场软件运维工作，包括日常巡检、例行维护、数据运维、响应式维护、故障处置、技术支持等。
6	硬件运维工程师	负责现场前端硬件设备的运维工作，包括日常巡检、例行维护、故障处置、技术支持等。
7	安全工程师	负责安全运维工作，包括权限管管理、漏洞扫描、渗透测试、安全评估、安全审计、应急演练、重要时期保障、信息安全培训等。

五、运维管理要求

运维团队需接受项目业主单位的全程监督与考核。依据运维服务合同及相关管理制度，对运维团队的服务质量、响应时效、工作规范性等进行定期检查与评估。

同时运维团队内部建立考核机制，明确考核要求及内部奖惩机制，确保运维服务质量持续提升。

所有运维人员入场前签署保密协议，明确保密责任和义务。运维人员需接受保密教育培训，学习保密法律法规、保密制度规定等。日常工作中，运维人员要严格遵守保密纪律，禁止私自复制、存储、传输涉密信息，禁止在社交媒体或非工作场合讨论项目敏感内容。

运维团队人员需保持稳定，不得随意更换，若需更换需提前 30 个日历日向甲方提交书面申请，经同意后方可更换，且更换人员资质不低于原人员。

严格执行汛期运维要求，强化监控与应急处置，支撑核心业务稳定运行。

运维团队需完成用户临时交办的其他维护任务。

六、运维服务体系

1.运维主要内容

（1）平台业务应用系统软件运维：维护各类业务功能模块的正常运行，包括功能验证、错误修复、版本迭代更新、用户需求响应等。维护频次取决于软件发布周期和问题报告的实际情况，包含定期更新和不定期的故障应急响应。

（2）数据库运维：执行数据库备份恢复计划、进行性能监测与优化、SQL 查询分析、空间管理和数据清洗等工作。数据库维护执行每周的备份计划，每季度定期进行性能调优和完整性检查。

（3）操作系统运维：监控操作系统的健康状况，进行系统补丁更新、安全加固、故障排查和性能调优，确保系统高可用性。维护频次每月进行例行检查，紧急安全更新则需要实时响应。

（4）网络设备运维：管理和维护网络设备的正常运行，包括交换机、服务器等。定期检查和更新网络设备的软件和硬件，确保网络的安全和稳定。同时，对网络带宽和流量进行监控，避免网络拥堵。

（5）网络硬盘录像机运维：监控录像机的存储状态，确保录像数据完整且未被篡改；检查网络连接状态，确保录像数据能够实时上传和下载；定期检查录像质量和分辨率。定期对硬盘进行健康检查，必要时进行更换；确保录像机软件的更新和维护；定期检查网络连接设备，如交换机、路由器等。

（6）防火墙运维：监控网络流量，识别异常行为；定期检查防火墙规则，确保其符合安全策略；监控防火墙日志，发现潜在的安全威胁。更新防火墙固件和安全策略；定期进行防火墙性能测试；确保与其他安全设备的协同工作。

（7）视频监控运维：对监控摄像头的工作状态，包括图像质量、云台控制、红外夜视功能等进行定期巡检，保证视频监控效果；对太阳能板、蓄电池以及市电接入线路、配电设备定期巡检，发现问题及时处理。对光纤网络通信设备进行定期巡检，确保网络通信传输可靠。定期清洗镜头、调整焦距，检查电源线和信号线，确保视频采集的连续性和清晰度。

2.运维管理制度建设

运维团队需遵照国内外相关运维标准，结合目前的实际情况，统一制定运维管理制度和规范。通过定期和不定期的检查，促进各项制度规范的贯彻落实，从而建立起全局统一、规范的运行维护管理工作方式。同时，随着西安市水务局信息化建设的不断发展，也要确保各项制度的及时更新。制度体系内容要涵盖资产管理、主机和应用管理、存储和备份管理、技术服务管理、安全管理、文档管理以及人员管理等类别。各类制度具体内容因需要而定，如网络管理制度需覆盖网络的接入管理、用户管理、配置管理及网络日常运行管理和应急处理等。安全管理制度需覆盖包括网络、主机、数据库、中间件、应用软件、数据信息的安全管理、其他机密资源和人员的安全管理以及安全事件的应急处理等。

3.运行维护管理流程

为加强运行维护管理，确保运行维护体系高效、协调运行，运维团队应依据运维管理环节、管理内容、管理要求制定统一的运行维护工作流程，实现运行维护工作的标准化、规范化和自动化。通过建立运维管理流程，可以使日常的运维工作流程化，职责角色更加清晰，从而使解决问题的速度和质量得到有效提高，实现知识积累和知识管理，并可以帮助运维部门进行持续的服务改进，提高服务对象的满意度。运行维护流程包含的环节有事件管理、问题管理、变更管理及配置管理。

（1）事件管理

事件是指在运行维护服务中不属于标准操作的并能导致或可能导致服务的中断或服务质量下降的任何事件。事件不仅包括了软件和硬件有关的错误，也包括服务请求。

事件管理负责对事件处理过程进行监控，并根据事件影响程度决定服务等级或应急响应等级的调整。事件管理涉及的范围应包括故障处置、应急响应等运行维护活动。

事件管理过程应包括事件受理、初步诊断和分类、解决、进展监控与跟踪、关闭等关键过程节点。实际应用中可根据自身实际情况，在关键节点基础上调整相应管理节点。

事件过程管理包括下列内容：

a) 建立事件分类分级机制，根据事件故障影响程度确定事件等级，并启动相应处理流程。

b) 在事件处理完毕后，与事件影响的用户确认事件处理完成情况，并加以记录。

c) 在事件处理过程中，若需要修改系统相关配置，应适时启用变更管理流程，保证相关记录与运行维护服务对象运行配置相一致。

d) 建立事件评估机制，包括事件分类、事件解决情况统计、事件解决时间统计、事件影响程度分析等，为提升运行维护服务质量提供依据。

e) 事件处理过程中产生的文档、记录等及时归档。

（2）问题管理

问题管理是通过调查所有可用信息，来确定引起事件发生的真正潜在原因以及提供的服务中可能存在的故障。

问题管理与事件管理的区别在于事件管理的目标是采取任何可能的方法快速地解决事件，而问题管理则注重确定并消除引起事件和问题的深层原因。事件管理是问题管理的重要的信息提供者，问题管理则支持事件管理流程的工作。

a) 问题识别和提交

问题提交者根据问题识别策略识别问题，并在系统中提交问题。问题类型至少包括：

1) 运行维护服务人员日常维护工作中针对隐患或弱点提出的问题；

2) 运维负责人和问题处理人在事件/问题趋势分析等问题管理活动时提出的问题。

b) 问题分类和分配

1) 运维负责人对提交的问题进行分类和优先级排序；

2) 运维负责人根据问题类别和优先级指派解决该问题的处理人。

c) 问题解决

1) 问题处理人判断该问题是否是自己解决范围内的问题，如果不是自己解决范围内的问题，则退回给运维负责人；

2) 问题处理人根据问题的优先级处理问题进行根源分析，在系统或表格中记录问题根源、临时解决方案和最终解决方案，更新已经查找到根源且具备解决方案的问题状态；

3) 若问题的解决方案需要通过变更实现，则提交变更请求，进入变更管理流程；

4) 问题解决后将解决方案告知相应的问题提交者和运维负责人。

d) 问题关闭

1) 运维负责人决定问题是否可以关闭。问题关闭前检查解决方案是否记录完整，如果不完整则要求问题处理人补充完整；

2) 查看问题的分类是否正确，如不正确，则由问题经理予以纠正；

3) 检查问题是否彻底解决，如果未彻底解决，则重新进入问题解决流程；

4) 问题关闭前需得到问题提交者的认可。

（3）变更管理

变更管理的目标是管理变更的过程，确保标准方法和过程可以得到使用，使得变更可以快速、对服务质量影响最小地得到处理，并保证所有的变更都可以被追踪。

变更经常会引起一系列应用系统或者技术架构的开发和分发。许多影响信息系统或处于同一影响范围的变更会被整合到一个包发布，由发布管理统一管理。

变更管理是对变更过程进行监控。变更管理包括例行维护、响应式维护、故障处置、应急响应、安全管理等。

变更管理过程应包括变更请求、评估、审核、实施、确认和审计等关键过程节点。变更过程管理应做到下列几点 ：

a） 根据变更类型和变更的范围进行变更评估。

b） 根据紧急程度、业务影响度等将变更分为常规变更、重大变更、紧急变更三种类型。常规变更指的是频繁发生、影响范围较小、紧急程度较低、实施风险较小、已经制定了标准实施流程的变更；重大变更指的是实施工作复杂、影响范围广、存在风险、需要制定详细方案、在系统与业务功能方面有重大调整的变更；紧急变更指的是如果不进行变更，会立即严重影响业务运行、导致服务等级收到严重影响的变更。

c） 变更方案应包括回溯机制。

d） 变更管理应保证相关记录与运行维护服务对象运行配置一致，目的是确定所需要的变更，并使这些变更在最小的范围内得到实施。

e） 配置项应包括运行维护服务对象的硬件、网络、软件、应用、环境、系统及相关文档的配置情况。

（4）配置管理

配置管理是指识别和确认系统的配置项、记录和报告配置项状态和变更请求、检验配置项的正确性和完整性等活动构成的服务管理流程。

在配置管理中，最基本的信息单元是配置项。所有软件、硬件和各种文档，比如变更请求、服务、服务器、环境、设备、网络设施、台式机、移动设备、应用系统、协议、电信服务等都可以被称为配置项。所有有关配置项的信息都被存放在运行维护台账中。运行维护台账不仅保存信息系统基础架构中特定组件的配置信息，而且还包括各配置项相互关系的信息。运行维护台账需要根据变更实施情况进行不断的更新，以保证配置管理中保存的信息总能反映信息系统基础架构的现时配置情况以及各配置项之间的相互关系。

a） 配置管理规划

根据配置请求确定配置的范围并制订配置计划，分配配置管理员。

b） 配置项识别

配置管理员定义配置项类别、标识、属性及其关系，识别配置项，提交运维负责人审核。通过审核后，配置管理员记录配置项信息，并添加至运行维护台账。

c） 运行维护台账控制

配置管理员负责维护配置项信息，并定期审查配置数据库，确保其正确性。

d） 运行维护台账审计

运维负责人组织配置项审计计划，根据计划审计配置项信息，编写审计报告。

e） 配置管理回顾及改进

定期生成配置管理报告，并召开会议讨论，发现弱点并进行改进。

4.工具装备

运维团队需配备必要的工具、设备，确保运行维护工作安全、有序、高效开展。包括但不限于以下：

交通工具：SUV 工程车，用于装载工具和人员通行。

安全防护装备：

安全帽、反光背心、防滑劳保鞋

救生衣（靠近水域作业必须）

手套（防割、绝缘）

安全带/安全绳（用于攀登水位计塔、流量塔）

通用工具：

综合工具套装（螺丝刀、扳手、钳子、内六角等）

万用表（数字式）、钳形电流表

兆欧表（测量绝缘电阻）、接地电阻测试仪（检查防雷设施必备）

手电筒、头灯（强光）

无人机（可选，用于巡查下河道路、断面标志及高风险水域）

通信与电子工具：

笔记本电脑（安装设备配置软件）

SIM 卡测试仪、移动 Wi-Fi 热点

对讲机（用于现场通信）

卷尺、激光测距仪

备用蓄电池、太阳能控制器、保险丝、连接线缆等常用耗材。

2.2 软件运维

软件运维内容主要包括日常监控巡检、例行维护、数据运维、响应式维护、故障处置、技术支持与服务，具体内容如下：

2.1.1 日常监控巡检

（1）巡检频次

非汛期对软件平台每日开展 1 次全面巡检，汛期每日开展 2 次全面巡检。汛期、强降雨、重要保障时期等特殊时段，加强监控巡检。

（2）巡检内容

核查软件平台整体运行状态，确保系统功能正常；

检查系统日志、告警信息，实时排查运行异常、服务中断、数据延迟等隐患；

监控服务器性能、网络状态、应用服务响应效率，保障系统运行流畅；

核验数据接收、模型推演计算、结果输出全链路通畅性，确保数据及时准确。

日常监控巡检			
工作步骤	**工作内容**	**工作标准**	**交付物**
启动巡检程序	确认巡检时段，打开巡检台账，记录巡检时间、巡检人员。	非汛期每日至少 1 次、汛期每日至少 2 次。	《日常巡检记录表》（每日填写）《巡检问题记录》（如有异常）
系统运行状态检查	访问软件平台主界面，验证核心功能页面可正常加载，依次检查各业务模块功能可用性。	根据软件巡检清单逐项检查各功能点状态，形成记录。	
日志与告警信	登录系统日志管理平台，查看当日系统日志，	保留异常日志、告警记	

息检查	检查告警列表，对异常告警进行初步分析、处置。	录。	
服务器性能监控	检查服务器 CPU、内存、磁盘使用率，监控网络连通性与带宽占用情况，检查应用服务响应时间。	根据服务器清单逐项检查并记录。	
数据链路检查	检查数据接收接口是否正常获取外部数据，验证模型推演计算任务的执行状态，确认结果输出接口数据是否及时准确。	根据数据接口清单逐项检查并记录。	

2.1.2 例行维护

（1）定期开展软件平台全维度健康检查，覆盖系统运行、服务调用、数据交互、性能负载等核心维度；

（2）按计划完成软件补丁升级、版本更新、性能调优，提升系统运行效率与稳定性；

（3）开展数据库日常维护，优化数据存储结构，提升数据读写效率；

（4）做好系统日志归集与分析。

例行维护			
工作步骤	**工作内容**	**工作标准**	**交付物**
系统健康检查	全面检查软件运行健康状态，覆盖系统运行、服务调用、数据交互、性能负载，记录检查结果，每月开展一次。	覆盖全面，记录完整。	《系统健康检查报告》（每月）
软件补丁升级与版本更新	制定升级计划，明确升级时间窗口，在测试环境验证补丁/版本的兼容性，执行升级操作，按需开展。	严格按照计划进行软件升级与更新，做好应急措施，保障业务连续性。	《软件升级记录表》（每次升级）
性能调优	分析系统性能监控数据，定位性能瓶颈，优化配置参数、数据库索引、缓存策略，验证调优效果，按需开展。	保留性能瓶颈、异常记录，记录性能调优。	《性能调优方案及验证报告》（每次调优）
数据库日常维护	执行数据库碎片整理，检查索引有效性并重建失效索引，更新统计信息，清理历史数据释放存储空间，每月开展一次。	记录异常信息，清理前做好数据备份。	《数据库维护记录表》（每月）
系统日志归集与分析	导出系统日志，对日志进行分类归档，分析日志中的异常模式，形成日志分析报告，每月开展一次。	保留异常日志，记录分析方法。	《日志分析报告》（每月）

2.1.3 数据运维

（1）完成内外部数据的对接、同步与日常维护；

（2）按要求完成数据备份，定期检查备份情况并进行数据恢复测试；

（3）开展数据治理工作，围绕数据采集、传输、存储、处理、应用、销毁等全生命周期开展治理活动，确保数据质量符合业务要求；

（4）按业务需求规范执行数据添加、修改、删除、导出等操作，保障数据合规使用。

数据运维			
工作步骤	**工作内容**	**工作标准**	**交付物**
数据对接与同步	检查内外部数据源连接状态，执行数据同步任务，监控同步进度与结果，处理数据同步失败或异常情况	记录同步失败及异常情况，每日形成数据检查记录。	《数据检查记录》
数据备份	制定数据备份计划，明确备份频率与保留策略，执行全量备份与增量备份，定期检查备份文件的完整性	每周检查备份情况	《数据备份与恢复测试报告》
数据恢复测试	制定数据恢复测试计划，在测试环境中执行数据恢复操作，验证恢复后数据的完整性与可用性	每年组织一次数据恢复测试	
数据操作管理	接收并审核数据添加、修改、删除、导出需求，	记录操作内容与时间，	《数据治理报告》

	按规范执行数据操作	定期审计数据操作记录	
数据治理	围绕数据采集、传输、存储、处理、应用、销毁等全生命周期开展治理活动，确保数据质量符合业务要求	每季度形成数据治理报告	
模型数据率定及校验	每日检查专业模型的自动运行状态，验证模型输入数据的完整性与及时性，确认模型输出结果的正常生成； 完成模型参数率定、校验、算法优化，提升模型效能。	每日记录模型运行情况，每次模型率定、校验、优化后形成报告	《模型运行监控日志》 《模型参数率定报告》 《模型校验报告》 《模型算法优化方案及效果报告》

2.1.4 响应式维护

（1）依据水务业务实际需求，完成系统配置变更、权限调整、业务流程优化等工作；

（2）做好维护过程记录，留存操作日志、现场资料，确保维护流程可追溯、可核查；

（3）响应时间小于 30 分钟。

响应式维护			
工作步骤	**工作内容**	**工作标准**	**交付物**
需求接收与评估	接收用户系统配置变更、权限调整、业务流程优化需求，评估需求的技术可行性与工作量，制定维护方案并明确实施计划。	记录用户需求并签字确认。	《维护需求评估表》（每次需求）
变更实施	在测试环境验证变更方案，在生产环境执行变更操作，验证变更效果确保业务正常运行。	变更实施前进行充分测试。	《变更实施记录表》（每次变更）
问题修复与功能完善	收集用户反馈的问题与改进建议，定位问题根因并制定修复方案，实施代码修复或算法升级，进行功能测试与回归测试。	记录问题内容、原因、修复方法。	《问题修复报告》（每次修复）
维护记录留存	记录维护过程（包括操作步骤、变更内容、测试结果），保存操作日志、现场截图等资料，归档维护文档确保可追溯。	保留维护记录，每月汇总提交。	《维护档案包》（包含操作日志、现场资料等）

2.1.5 故障处理

（1）系统故障发生后，30 分钟内完成响应，60 分钟内出具故障初步研判结果。需现场处置的故障，接到通知后 1 小时内抵达现场开展处置工作。

（2）一般故障：2 小时内完成排查与修复，恢复系统正常运行。重大故障：6 小时内完成全面处置，消除故障影响，保障业务连续。如预计无法按时完成情况，由运维团队向用户提交延期申请，审核通过后按期尽快完成修复。

（3）按规范完成故障定位、原因分析、问题修复、效果验证全流程，输出事件处理文档与标准化解决方案，形成故障处置闭环。

（4）建立并维护故障知识库，每次故障分析报告完成后，更新知识库。

故障处理			
工作步骤	**工作内容**	**工作标准**	**交付物**
故障响应与初步研判	接收故障报告确认故障级别，30 分钟内响应，60 分钟内完成初步研判，判断故障性质并确定处置方案	记录故障响应时间及内容	《故障处置报告》（每次故障）
现场处置	接到通知后 1 小时内抵达现场，现场排查故障根因，执行应急恢复措施	留存现场照片记录	
故障定位与修复	一般故障 2 小时内完成排查与修复，重大故障 6 小时内完成全面处置，验证修复效果确认系统功能恢复正常	故障修复后进行验证确认	
故障分析与总结	分析故障根因形成故障分析报告，制定标准化解决方案与预防措施，更新故障知识库	记录故障情况、原因、并形成相应知识	
故障闭环	输出事件处理文档，确认用户满意度，归档	每月汇总提交	

	故障处置资料		

2.1.6 技术支持与服务

（1）提供 7×24 小时服务热线、远程技术支撑与现场维护服务，全天候响应水务业务运维需求；

（2）为用户提供系统应用咨询、预报结果解读、数据分析等专业技术支撑；

（3）为系统用户提供基础操作指导、常见问题解答及数据调用支持服务；

（4）开展系统操作培训、业务应用培训，提升用户系统使用能力与业务处理效率。

（5）如遇重大故障或疑难问题，需免费提供原厂服务。

技术支持与服务			
工作步骤	**工作内容**	**工作标准**	**交付物**
服务响应	7×24 小时接听服务热线，记录用户问题描述与需求，根据问题类型分配技术人员	及时响应，详细记录。	《技术服务工单》（每次服务）
远程技术支撑	通过远程工具诊断系统问题，指导用户进行问题排查，无法远程解决时安排现场支持	记录远程技术支持过程	
专业技术支撑	为用户提供系统应用咨询，解读预报结果提供数据分析服务，协助用户制定业务解决方案	形成解决方案成果	
基础操作指导	指导用户进行系统基础操作，解答常见问题（FAQ），协助用户进行数据调用	每次进行记录	
培训服务	制定培训计划与培训材料，开展系统操作培训和业务应用培训，评估培训效果	形成佐证材料。	《培训报告》（每次培训，包括培训通知、培训材料、培训记录等）

2.1.7 运维管理要求

（1）建立标准化巡检台账，每日如实填写巡检记录，每月提交《运维总结报告》，根据甲方要求细化运维方案及成果文档并开展工作。

（2）遵循水务行业信息化运维规范，执行标准化作业流程，保障运维工作合规、高效。

（3）强化业务协同，配合防汛调度、水资源管理、大坝安全监管等业务工作，提供精准运维支撑；

（4）持续优化运维方案，结合水务信息化系统升级、业务拓展需求，同步更新运维工作内容与标准。

（5）构建专业化运维团队，团队成员需全面掌握系统的技术架构、设备原理及业务逻辑。定期开展技术培训与业务交流，确保团队成员精通系统操作、故障排查及应急处理，能够精准响应各类运维需求，为系统稳定运行提供坚实的人力支撑。汛期驻场 3 人，非汛期驻场 2 人，参与值班保障。

（6）严格把控数据从采集、传输到存储、分析的全生命周期质量。要求数据采集及时，确保各类监测数据实时上传，无遗漏；保证数据准确，通过多源数据比对、自动校验及人工复核相结合的方式，避免数据失真、错误或异常值，为防汛调度决策提供可靠的数据依据。

（7）针对汛期、国家法定节假日及其他重要时期，根据需求驻场提供技术支撑保障工作，确保系统正常稳定运行。

（8）维护软件所支出的费用以及各应用系统日常问题处理支出(主要包括软件日常维护、数据维护、安全维护以及现有功能的优化完善),包含定制软件系统和通用软件(如存储系统、操作系统、中间件等)。

（9）安全运维服务:对保障信息系统安全相关的安全产品(包含数据库安全审计、防火墙、安全网关、态势感知、应用防护、检测管理等)续保费用,软硬件实施例行操作、响应支持、调研评估和优化改善等服务,如监测预警及应急响应、防护加固。

2.2 硬件运维

硬件运维内容主要包括日常监控巡检、例行维护、响应式维护、故障处置，具体内容如下：

2.2.1 日常监控巡检

（1）巡检频次

在线状态监控：非汛期每日 1 次核查设备在线情况，汛期每日 2 次；

现场定期巡检：前端监测站点、视频监控、网络通信、供电配套设备每季度 1 次现场巡检，并对影响设施设备的不利因素进行现场处置，例如修剪视频监控、太阳能板等周围遮挡树枝及杂物；计算机终端、存储设备每月 1 次现场维护；

专项周期巡检：定期核查网络设备系统版本与安全规则，检查视频监控画面，汛期对防汛关键硬件开展专项高频巡检。

（2）巡检内容

前端感知与视频设备：核查在线状态、画面清晰度与流畅度，确认录像存储与回放正常；检查太阳能供电、户外设备箱密封情况。（每季度）

网络与安全设备：监控交换机、路由器、防火墙、融合网关、视频工业级 4G 路由器等设备的运行状态，检查设备指示灯、告警信息，审计防火墙规则与异常流量，核查政务外网 IP、负载均衡、SSL/TLS 证书状态。（每季度）

服务器与存储设备：监控计算服务器、渲染节点工作站、区县采集服务器、硬盘录像机硬件性能、存储 IO、电源散热状态，保障数据库硬件连接稳定性。（每月）

供电与配套设备：检查电源稳压器、设备箱体完整性，排查物理损坏、过热、异响等问题，保障供电稳定。（每季度）

日常监控巡检			
工作步骤	**工作内容**	**工作标准**	**交付物**
在线状态监控	（1）执行设备在线状态核查 （2）检查所有前端感知设备、视频监控设备、网络设备在线状态。 （3）记录设备在线率、离线设备信息及原因分析。 （4)对离线设备进行标记并通知相关运维人员。	非汛期每日至少 1 次,汛期每日至少 2 次。每日形成检查记录。	《设备在线情况检查表》
现场巡检	（1）前端监测站点、视频监控、网络通信、供电配套设备，每季度 1 次现场巡检。 （2）存储设备：每月 1 次现场维护。 （3)到达现场后,逐一检查设备物理状态、运行指示灯、连接线路。 （4）执行设备清洁、紧固、调试等现场维护操作。	每次现场巡检留存照片记录，详细检查现场设备及周边环境，保障设备安全稳定运行。异常情况及时记录上报。	《设备巡检记录表》（每月/季） 《服务器运行监控记录》（每日）
专项巡检	（1)定期核查网络设备系统版本与安全规则配置。	根据用户需求进行专项巡检，记录巡检内容及异常情况。	

	（2）检查视频监控画面清晰度、流畅度及录像回放功能。 （3）汛期对防汛关键硬件开展专项高频巡检。 （4）形成专项巡检报告，记录发现的问题及整改建议。		
前端感知与视频设备	（1）核查设备在线状态，确认设备连接正常 （2）检查视频画面清晰度与流畅度，确认无明显卡顿、失真。 （3）测试录像存储与回放功能，确保录像完整可查。 （4）检查太阳能供电系统电压、电流状态，评估供电稳定性。 （5）检查户外设备箱密封情况，防止进水、进尘。	检查、调整前段监测设备状态，保障监测数据正常、准确。 检查视频监控周围环境，清理遮挡，保障画面清晰、完整。	
网络与安全设备	（1）监控交换机、路由器、防火墙、融合网关、视频工业级 4G 路由器等设备的运行状态。 （2）检查设备指示灯状态，查看告警信息及日志。 （3）审计防火墙规则配置，检查异常流量记录。 （4）核查政务外网 IP 分配与使用情况。 （5）检查负载均衡设备运行状态及流量分发情况。 （6）核查 SSL/TLS 证书有效期及配置状态。	详细记录网络设备配置更改、策略调整内容。 建立证书台账，提前申请、更新，避免证书过期。	
服务器与存储设备	（1）监控服务器硬件性能指标（CPU、内存、磁盘使用率）。 （2）监控区县采集服务器连接状态及数据采集情况。 （3）检查硬盘录像机存储容量、录像完整性。 （4）监控存储设备 IO 性能及响应时间。 （5）检查电源、散热系统运行状态，确保温度在正常范围。 （6）确认数据库硬件连接稳定性。	记录服务器及存储设备检查结果，异常情况及时上报。	
供电与配套设备	（1）检查电源稳压器输入输出电压是否稳定。 （2）检查设备箱体完整性，无变形、破损。 （3）排查设备是否存在物理损坏、过热、异响等问题。 （4）检查供电线路连接是否牢固，无老化、破损。 （5）保障供电稳定性，确认备用电源设备正常。	严格执行安全生产要求，保障运维过程人员安全。	

2.2.2 例行维护

（1）设备清洁保养

每季度清洁设施设备灰尘，擦拭摄像头镜头与外壳、加固支架，调试视频监控点位角度与焦距。

（2）硬件性能优化

测试校准电源稳压器输出电压，优化防火墙规则、路由策略、安全策略，关闭风险端口；提升服务器、存储 IO 性能，确保网络响应时间符合要求。

（3）系统固件维护

完成服务器的系统安全加固、内核优化与补丁更新，及时升级网络设备、网关、路由器安全补丁与系统版本，定期备份网络设备配置文件。

（4）预防性维护

定期更换设备老化部件，排查硬件隐患，避免因部件老化引发故障。

例行维护			
工作步骤	**工作内容**	**工作标准**	**交付物**
设备清洁保养	（1）每季度对所有设施设备进行灰尘清洁。 （2）擦拭摄像头镜头与外壳，确保画面清晰。 （3）加固摄像头支架，检查固定螺栓紧固情况。 （4）调试视频监控点位角度与焦距，确保监控范围合适。 （5）清洁机箱内部灰尘，检查风扇运转情况。	设备清洁前断电，清洁后检查设备数据传输情况。	《设备清洁保养记录表》（每季度）
硬件性能优化	（1）测试校准电源稳压器输出电压，确保电压稳定在额定范围。 （2）优化防火墙规则，删除无效规则，优化规则匹配顺序。 （3）优化路由策略，调整路由表，减少不必要的路由跳转。 （4）优化安全策略，关闭风险端口，限制不必要的服务。 （5）提升服务器、存储设备 IO 性能，优化磁盘读写策略。 （6）测试网络响应时间，确保符合业务要求。	详细记录规则、策略修改内容。	《硬件性能优化方案》（每次优化）
系统固件维护	（1）完成服务器等设备的系统安全加固。 （2）优化服务器内核参数，提升系统性能。 （3）安装系统安全补丁与功能更新。 （4）升级网络设备、网关、路由器安全补丁与系统版本。 （5）定期备份网络设备配置文件。 （6）验证升级后设备功能正常，无兼容性问题。	固件维护前进行测试验证，保证设备稳定性。	《系统补丁升级记录表》（每次升级）
预防性维护	（1）定期检查设备老化情况，制定部件更换计划。 （2）更换老化、有故障风险的硬件部件（如硬盘、风扇、电源等）。 （3）排查硬件隐患，检查设备运行异常记录。 （4）预防性更换即将过期的配件（如电池、线缆等）。 （5）记录预防性维护情况，形成维护台账。	制定预防性维护计划，经业主单位审核通过后进行设备维修、配件更换等。	《部件更换记录表》（每次更换）

2.2.3 响应式维护

（1）配置与参数调整

根据业务需求完成硬件配置变更、设备信息更新、监控参数调试。

（2）策略与证书管理

优化网络策略、更新 SSL/TLS 证书、完善安全策略。

响应式维护			
工作步骤	**工作内容**	**工作标准**	**交付物**

配置与参数调整	（1）接收业务部门硬件配置变更需求。 （2）评估变更需求的可行性与影响范围。 （3）在测试环境验证配置变更方案。 （4）在生产环境执行硬件配置变更。 （5）更新设备信息登记，调整监控参数阈值。 （6）验证变更效果，确保设备正常运行。	记录变更需求内容、评估、方案、变更过程、验证结果。	《配置变更记录表》（每次变更） 《网络策略优化方案》（每次优化） 《证书更新记录表》（每次更新）
策略与证书管理	（1）评估现有网络策略的合理性。 （2）根据业务需求优化网络策略、安全策略。 （3）检查 SSL/TLS 证书有效期，提前 30 天预警。 （4）更新即将到期的 SSL/TLS 证书。 （5）验证新证书部署生效，无访问异常。 （6）完善安全策略，封堵新增的安全风险点。	记录、备份原有策略、证书、规则。记录修改内容。	

2.2.4 故障处理

（1）针对硬件设备提供故障处置服务，设备发生故障时，在规定的时间内消除故障影响并最终清除故障。故障发生 30 分钟内响应，汛期城区 3 小时内人员到达现场，非城区 6 小时到达现场。非汛期 6 小时内人员到达现场。故障排除时间汛期不超过 8 小时，非汛期不超过 24 小时。

（2）详细记录故障时间、设备名称、现象、排查过程与处理结果，形成处置闭环。

（3）每月汇总分析故障数据，定位频发问题，制定预防性措施，降低故障发生率。

故障处理			
工作步骤	**工作内容**	**工作标准**	**交付物**
故障处置服务	（1）接收硬件设备故障报告，确认故障等级。 （2）30 分钟内响应，开始初步故障诊断。 （3）汛期 3 小时内、非汛期 6 小时内人员到达现场（城区）。 （4）现场排查故障原因，制定处置方案。 （5）执行故障修复操作。 （6）汛期 8 小时内、非汛期 24 小时内完成故障排除。 （7）验证设备恢复正常运行。	记录故障时间线、内容、修复情况。	《故障响应记录表》（每次故障） 《故障修复记录》（每次故障） 《故障处置报告》（每月）
记录与闭环	（1）详细记录故障发生时间、设备名称、型号。 （2）记录故障现象及用户描述。 （3）记录排查过程、诊断结果及处理措施。 （4）记录故障修复结果及验证情况。 （5）形成故障处置闭环文档。 （6）更新故障知识库。	故障闭环管理，提交完整记录。	
汇总分析	（1）每月汇总所有硬件故障记录。 （2）分析故障类型分布（设备类型、故障原因）。 （3）定位频发问题，识别高故障率设备或部件。 （4）分析故障原因，找出根本原因。 （5）制定预防性措施和改进方案。 （6）更新预防性维护计划。	成果纳入知识库，提交业主单位。	

2.2.5 运维目标与指标

（1）视频监控系统可用率≥98%；整体硬件设备在线率≥95%，设备完好率≥95%。

（2）网络响应时间持续低于 200ms；视频图像清晰无卡顿、黑屏、雪花、偏移。

（3）定期完成漏洞修复与策略优化，全年无重大硬件及网络安全事故。

2.2.6 运维管理要求

（1）现场巡检填写记录并拍摄现场照片，建立巡检、故障、配置变更、维修更换完整运维台账。

（2）每季度提交巡检及故障处置报告，每年提交《硬件运维总结报告》，根据甲方要求细化运维方案及成果文档并开展工作。

（3）严格执行汛期硬件运维专项要求，强化关键设备监控与应急处置，支撑核心业务。

（4）遵循水务信息化硬件运维标准，全程留存运维资料，确保运维过程可追溯、可核查。

（5）完成用户临时交办的其他维护任务。

（6）维护软件所支出的费用以及各应用系统日常问题处理支出(主要包括软件日常维护、数据维护、安全维护以及现有功能的优化完善),包含定制软件系统和通用软件(如存储系统、操作系统、中间件等)。

（7）安全运维服务:对保障信息系统安全相关的安全产品(包含数据库安全审计、防火墙、安全网关、态势感知、应用防护、检测管理等)续保费用,软硬件实施例行操作、响应支持、调研评估和优化改善等服务,如监测预警及应急响应、防护加固。

2.2.7 硬件运行维护周期及标准

物理资源								
类别	**对象**		**项目**	**检验标准**	**周期**			
					日常	**月度**	**季度**	**年度**
视频监控硬件维护	外观及接口		清洁、除尘、防静电、紧固	干净整洁、无异味、无短路、无接触不良	√			
	视频监控硬件维护	主机	运行工况调整、完善	运行正常		√		
		视频监控头（机）	视频监控质量检测	器件灵敏度、画面清晰度（不同照度情况下）符合要求		√		
			防潮、防尘、防腐维护	达到三防要求		√		
		云台控制器	云台定期维护	正常运行		√		
		编解码器	接口测试	测试正常		√		
		屏幕	屏幕校验	检测正常		√		
		存储设备	空间、性能检查测试	未达到警戒容量、性能正常		√		
		视频交换机	各端口网线连接检查	连接牢固，无松动，无故障		√		
		视频光端机	传输光衰检查	传输损耗应在视频光端机接收灵敏度范围内		√		
	系统维护		系统整体调测	系统正常		√		
			联动测试	测试正常				
网络系统	外观及接口		清洁、除尘、防静电、紧固	干净整洁、无异味、无短路、无接触不良	√			
	网络设	路由器	接口测试；检查数据流量、系统利用率等参数；访问控制列表检测	正常运行		√		

	备维护	交换机	接口测试；系统硬件验证、调试；vlan 检测	正常运行		√		
		无线网络设备	接口测试；调试速率、参数调整	测试正常		√		
	系统维护		网络运行健康监测	监测分析	√			
			设备基础运行性能检测	监测分析	√			
			网络拓扑链路状态监测	监测分析	√			
			资源开销监测与管控	监测分析	√			
			网络优化与改善	优化改善维护实施		√		
			主备切换与应急演练	正常实施		√		
计算存储系统	外观及接口		清洁、除尘、防静电、紧固	干净整洁、无异味、无短路、无接触不良	√			
	计算存储设备维护	服务器	CPU 峰值资源使用检测	检测正常		√		
			内存峰值资源使用检测	检测正常		√		
			硬盘空间检测	检测正常		√		
		存储服务器	服务器硬盘 RAID 保护调整与容量调整	调整后运行检测正常		√		
		磁盘阵列	读写高速缓存（Cache）比例调整；RAID 保护级别调整；	调整后运行检测正常		√		
	系统维护		系统日常监测	运行日志填写	√			
			控制器、硬盘等部件的微码升级	升级后运行检测正常		√		
			系统软件、管理软件的版本升级	升级后运行检测正常		√		
安全系统	外观及接口		清洁、除尘、防静电、紧固	干净整洁、无异味、无短路、无接触不良	√			
	安全设备维护	防火墙	接口测试；日志分析；网络安全事件检查；安全策略调整；网络安全风险分析；防火墙硬件升级	测试、调整后满足安全需求		√		
		VPN 设备	接口测试、通道质量测试	调整后满足专网优化需求		√		
	系统维护		安全系统运行监测	运行日志填写	√			
			安全事件监测和处置	处置后安全运行	√			
			安全事件周期性分析和改善	优化改善后满足安全运行需求		√		
			系统性升级	升级后正常运行		√		
	视频监控设施	供电系统	风光互补供电系统风机、太阳能电池板、支撑牢固等运行检测	风机运行正常、太阳能电池板无损坏，支撑牢固			√	
			POE 供电系统电压、供电模块检测	电压稳定达标			√	
			近地直供供电系统	配电安全，运行正常			√	
		无线传输系统	信号和传输质量测试	测试正常			√	
		光纤传输系统	视频光端机发光功率测试	发光正常			√	
			打环测试收光功能	收光正常			√	
			传输损耗测试	传输损耗应在视频光端机接收灵敏度范围			√	

	系统维护	系统整体调测	系统正常		√		
		联动测试	测试正常		√		
注：（硬件设备现场巡检及维护可参照本表，不局限于本表内容。）							

2.3 安全运维

西安市水务局严格执行《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律法规要求，以网络安全等级保护制度为基本遵循，全面落实党委（党组）网络安全工作责任制，切实履行网络安全主体责任。为加强网络安全工作的组织领导，我局成立了网络安全和信息化工作领导小组及网信工作专班，明确由局党组统一领导、网信专班具体负责、各业务部门协同配合的网络安全管理架构。

在制度建设方面，我局建立了网络安全管理制度体系，同时，严格落实网络安全等级保护制度，新增智慧水务平台、水灾害防御系统、水库大坝监测系统等关键业务信息系统，按照等级保护要求进行了定级备案、测评整改和安全加固，确保系统安全保护能力符合国家标准要求。安全运维服务:对保障信息系统安全相关的安全产品(包含数据库安全审计、防火墙、安全网关、态势感知、应用防护、检测管理等)续保费用,软硬件实施例行操作、响应支持、调研评估和优化改善等服务,如监测预警及应急响应、防护加固。

本次所申报项目的安全运维，主要从技术和业务角度开展安全运维工作保障信息系统安全稳定运行，具体如下：

安全运维工作内容

工作项	工作内容	工作频度	
一、权限管理			
1.权限体系维护	（1）遵循最小权限原则，梳理智慧水务平台、水灾害防御系统、水库大坝监测系统等业务系统的用户角色体系。 （2）按照业务角色（系统管理员、业务管理员、操作员、查询员等）分级分配系统、数据库、设备操作权限。 （3）制定权限管理规范，明确各级用户的权限范围和操作边界。 （4）实施三权分立（系统管理员、安全管理员、安全审计员） （5）建立权限变更审批流程，确保权限变更有据可查。	每季度开展 1 次	1 名初级安全类工程师、1 名中级安全类工程师
2.权限审计与清理	（1）每季度开展用户权限全面检查工作，检查权限分配的合理性和合规性. （2）配合用户部门完成权限回收，清理离职人员、调岗人员的系统访问权限。清理无效账户、僵尸账户，删除超过 90 天未登录的临时账户。 （3）配合用户定期更新用户口令，口令复杂度满足等保要求。 （4）建立权限审计台账，记录权限变更历史	每季度开展 1 次，每次 2 人天	
二、漏洞处置			
1.漏洞修复	（1）根据漏洞扫描报告，制定漏洞修复方案，明确修复优先级和时限。 （2）对高危漏洞 48 小时内完成修复，对中危漏洞 7 天内完成修复。 （3）整改完成后申请复扫，确保中高危漏洞全部清零。 （4）建立漏洞修复台账，记录漏洞修复过程和结果。	每季度开展 1 次，	1 名中级安全类工程师
2.持续漏洞监测	（1）实时跟进官方漏洞发布（国家信息安全漏洞共享平台等）。 （2）监控相关厂商安全公告，及时获取补丁信息。 （3）即时完成系统补丁升级、代码漏洞核查修复。 （4）建立漏洞信息库，记录漏洞发布时间、影响系统、修复措施。	每周 1 次漏洞信息收集和评估	
三、渗透测试			

1.测试后整改加固	（1）根据渗透测试报告，制定安全加固方案。 （2）对发现的漏洞进行修复，包括代码修改、配置调整、策略优化等。 （3）优化安全防护策略，提升系统整体安全防护能力。 （4）开展渗透测试复测，验证修复效果。	每年 1 次	1 名中级安全类工程师
四、等保与密评			
1.等级保护测评	（1）对已建成系统（智慧水务平台、水灾害防御系统、水库大坝监测系统）进行等保定级备案。 （2）配合测评机构开展现场测评，提供系统架构、网络拓扑、安全配置等相关资料。 （3）填写等保测评备案表，协助测评机构收集测评所需材料。 （4）根据测评结果，识别不符合项，制定整改方案。	每年 1 次	2 名中级安全类工程师
2.等保整改与复测	（1）根据等保测评发现的问题，制定详细整改方案。 （2）完成安全配置、漏洞整改、日志审计、安全策略等整改工作。 （3）配置安全设备（防火墙、入侵检测、堡垒机、审计系统等）。 （4）整改完成后申请复测评，确保系统达到等保要求。 （5）获取等保测评报告，完成等保备案。	每次测评后	
3.密码应用安全性评估	（1）对涉及密码应用的系统开展密评工作。 （2）配合密评机构开展现场评估。 （3）完成密码应用安全性评估整改，确保符合国家密码法规要求。 （4）建立密码管理制度，规范密码算法、密码产品、密钥管理。	每年 1 次	
五、应急演练	（1）每年开展 2 次网络安全应急演练。 （2）演练场景包括：DDoS 攻击、勒索病毒、数据泄露、系统入侵、恶意代码等。 （3）参演人员：信息中心工作人员、运维团队、相关业务部门。 （4）验证应急预案的有效性，发现应急预案的不合理和不顺畅之处。 （5）通过演练提升应急响应能力，检验协同配合机制。 （6）形成演练评估报告，总结演练经验，修订应急预案。	每年 2 次	1 名初级安全类工程师，1 名中级安全类工程师
六、重要时期安全保障			
1.重要时期保障前准备	（1）识别重要时期。 （2）制定重要时期网络安全保障方案，明确保障目标、保障措施、人员安排。 （3）下发重要时期网络安全保障通知到各区县、直属单位（履行行业监管职责）。 （4）对信息系统进行全面安全检查，包括：漏洞扫描、安全加固、设备巡检。 （5）清理不必要的服务端口和临时账户，加强系统安全防护。 （6）准备应急响应资源和备份系统，确保应急可用。 （7）开展重要时期前专项培训，提升应急响应能力。 （8）建立重要时期值班制度，明确值班人员、值班时间、值班职责。 （9）制定重要时期信息报送机制，确保信息及时上报。	每次重要时期前	1 名初级安全类工程师，1 名中级安全类工程师

2.重要时期保障值守	（1）安排专人 7×24 小时值班值守，确保网络安全事件及时发现和处置。 （2）每日对系统网络安全进行检查，包括：系统运行状态、网络流量、安全告警。 （3）密切监控系统安全事件，识别入侵攻击、非法访问、异常数据传输等行为。 （4）每日编制重要时期网络安全日报，上报局领导和相关部门。 （5）根据应急响应预案，及时处置网络安全事件，确保尽快消除影响。 （6）加强与网信办、公安网安等部门的沟通协调，及时上报安全事件。 （7）做好重要时期网络安全记录，包括：值班记录、检查记录、事件记录等。	重要时期值守 7×24 小时，约 4 次	
3.重要时期保障总结	（1）重要时期结束后，形成重要时期网络安全保障工作总结报告。 （2）总结保障工作成效、发现的问题、经验教训。 （3）分析安全事件发生原因，制定预防措施。 （4）优化应急预案和保障方案，提升保障能力。	每次重要时期后	
七、信息安全培训			
1.信息安全意识培训	**培训对象：**业务系统使用人员，包括局机关各处室、各区县水务局、直属单位相关工作人员 **培训内容：** 网络安全法律法规（《网络安全法》《数据安全法》《个人信息保护法》）、网络安全形势与案例、网络安全意识（密码安全、邮件安全、移动安全、办公安全）、常见网络攻击防范（钓鱼邮件、勒索病毒、社会工程学攻击）、个人信息保护、安全事件处置流程等。 **培训交付物：** 培训通知（培训前发布） 培训课件（PPT、视频等） 培训记录（签到表、照片、视频） 培训总结报告（培训后形成）	每次培训 4 人天	1 名初级安全类工程师，1 名中级安全类工程师

采购包 2（网络安全服务）：

2026 年度西安市水务局信息化系统运维项目（新增运维），本次运行维护项目核心目标是建立一个高效可靠的运维体系，保证全部运维对象处于高效稳定的运行状态，通过信息化手段为防汛指挥决策提供技术支撑，最大程度减少水灾害造成的损失，守护人民生命财产安全。主要内容为保障信息系统安全相关的安全产品(包含数据库安全审计、防火墙、安全网关、态势感知、应用防护、检测管理等)续保费用,软硬件实施例行操作、响应支持、调研评估和优化改善等服务,如监测预警及应急响应、防护加固。

本次所申报项目的安全运维，主要从技术和业务角度开展安全运维工作保障信息系统安全稳定运行，工作频度和人员配备不少于表格要求次数/数量，根据需要可增加频次和人员数量，具体如下：

安全运维工作内容

工作项	工作内容	工作频度	人员配备
一、漏洞扫描			
1.漏洞扫描	（1）每季度针对我单位所有业务系统提交专项安全漏洞扫描需求，制定漏洞扫描方案。 （2）准备扫描环境，评估扫描动作对业务系统的影响，确保不干扰正常业务。 （3）对智慧水务平台、水灾害防御系统、水库大坝监测系统等进行全量漏洞扫描。 （4）扫描范围包括：操作系统漏洞、数据库漏洞、中间件漏洞、应用系统漏洞、网络设备漏洞等。 （5）分析扫描结果，排除误报，验证漏洞真实性。 （6）形成漏洞扫描报告，明确漏洞等级、影响范围、修复建议。	每季度开展 1 次	1 名中级安全类工程师

	（7）在漏洞修复完毕后进行复测。		
二、渗透测试			
1.渗透测试	（1）针对智慧水务平台、水灾害防御系统、水库大坝监测系统等重要业务系统，每年组织至少 1 次渗透测试。 （2）模拟实战攻击场景，采用黑盒测试、灰盒测试、白盒测试等多种方法。 （3）对系统接口、数据库、网络边界、移动端 APP 等进行全面安全评估。 （4）挖掘潜在安全隐患，包括逻辑漏洞、业务漏洞、权限绕过等。 （5）验证漏洞的可利用性，评估漏洞的危害程度。 （6）编写渗透测试报告，明确漏洞描述、利用过程、危害评估、修复建议。	每年 1 次	1 名高级安全类工程师
三、安全评估			
1.网络安全风险评估	（1）每年开展 1 次网络安全风险评估，覆盖所有业务系统。 （2）评估内容包括：资产识别、威胁分析、脆弱性识别、风险计算。 （3）采用定性和定量相结合的方法，评估网络安全风险。 （4）形成网络安全风险评估报告，上报网信办备案。 （5）根据风险评估结果，制定风险处置措施。	每年 1 次	1 名初级安全类工程师，1 名中级安全类工程师
2.数据安全风险评估技术支撑服务	（1）提供技术支持服务，对重要业务系统开展数据安全风险评估。 （2）评估数据全生命周期安全，包括：数据采集、存储、传输、使用、共享、销毁。 （3）识别数据安全风险，包括：数据泄露、数据篡改、数据丢失、非法访问等。 （4）形成数据安全风险评估报告。	每年 1 次	
四、安全审计			
1.运维安全审计	（1）每年对运维服务商开展 1 次安全审计。 （2）审计内容包括：人员管理、制度执行、技术措施、安全事件、合规性等。 （3）检查运维服务商的安全资质、人员背景、安全培训情况。 （4）审计运维操作规范性，检查是否存在违规操作、越权访问等。 （5）验证安全措施的有效性，包括：漏洞修复、安全加固、监控告警等。 （6）形成运维安全审计报告，提出整改建议。	每年 1 次	1 名初级安全类工程师，1 名中级安全类工程师
2.合规性审计	（1）定期开展网络安全合规性审计，检查是否符合《网络安全法》《数据安全法》《个人信息保护法》等法律法规要求。 （2）检查是否符合等保、密评、网络安全责任制等政策要求。 （3）审计安全管理制度执行情况，检查制度落实是否到位。	每年 1 次	
五、信息安全培训			
1.信息安全技能培训	**培训对象：**运维团队内部人员、信息中心工作人员、运维相关技术人员 **培训内容：** 等保 2.0 标准解读与实施、漏洞扫描技术与方法、日志分析与安全审计、应急响应技术、安全加固技术、安全设备配置与管理等。 培训交付物： 培训通知（培训前发布） 培训课件（PPT、视频等） 培训记录（签到表、照片、视频） 培训总结报告（培训后形成）	每次培训 4 人天	1 名中级安全类工程师，1 名高级安全类工程师
六、应急演练	（1）协助、指导运维单位每年开展 2 次网络安全应急演练。 （2）演练场景包括：DDoS 攻击、勒索病毒、数据泄露、系统入侵、恶意代码等。	每年 2 次	1 名高级安全类工程师

七、重要时期安全保障	重要保障时期和上级攻防演练期间，提前做好应对，安排专人驻场，落实防范措施，确保安全。		1 名高级安全类工程师

四、考核指标

由西安市水务信宣中心组织绩效评价，按照《西安市信息化项目绩效评价管理办法（试行）》《西安市水务信息化设备设施及系统运行维护评价实施细则（试行）》要求执行。

4.1 绩效评价方式

绩效评价采取日常绩效评价和用户满意度评价相结合的方式进行。日常绩效评价按评价指标周期开展，评价结果采取累计扣分制；运维结束后对水务信息化设施设备及系统运维进行用户满意度评价，绩效评价结果为日常绩效评价结果和用户满意度评价结果的加权和，最后一次绩效评价以《西安市信息化项目验收实施细则（试行）》进行履约验收的结果为准。

用户满意度评价主要通过审议项目绩效报告、查阅资料、现场检查、评价打分等环节进行，日常绩效评价主要通过查阅资料、现场检查、随机抽查、评价打分等方式进行。

4.2 绩效评价内容

绩效评价内容应围绕服务交付、服务质量、资源管理、资金管理、风险管理 5 个方面开展。

（1）日常绩效评价

日常绩效评价由市水务信宣中心组织实施，采用双随机抽查。评价内容涵盖：人员配置、人员资质及安全生产、人员值班及保密制度、巡检计划落地情况、问题整改闭环、系统可用性，以及运维机构管理制度、应急管理制度、备品备件管理制度、知识库管理制度、电子台账检查、数据治理制度、网络安全管理制度落实情况。

（2）用户满意度评价

用户满意度评价由局网信专班牵头，市水务信宣中心组织各相关处室（单位）共同开展绩效用户满意度评价，并形成《用户评价反馈意见》。内容涵盖：应急响应速度、应急响应态度、人员配置储备、人员技术能力、故障修复质量、设备运行情况、数据成果提交、网络安全、用户主观满意度、反馈改进情况。

（3）绩效评价结果汇总

绩效评价结果总分 100 分，评分向下取整，绩效评价结果等于日常绩效评价结果乘以 30%加上用户满意度评价结果乘以 70%。

4.3 评价标准

绩效评价结果分为优秀、良好、合格、不合格四个档次。

安全风险隐患整改不彻底、安全责任未落实的，绩效评价结果下调一档。

发生下列情形之一的，认定为安全风险隐患整改不彻底、安全责任未落实：

（1）核心业务数据出现泄露、篡改或丢失，导致业务决策受影响。

（2）因运维不力或操作不当，导致核心信息化设备损坏、网络中断，或关键业务系统停运，造成水务运营调度受阻、应急响应延迟。

（3）设备或系统遭遇网络攻击，突破防护体系，或因安全漏洞未及时修复和违规操作，导致数据中心服务器瘫痪、核心数据库被篡改，造成敏感数据泄露量超过一定规模，造成社会不良影响。

（4）因运维人员操作不当，导致信息化设备运行维护过程中造成人员受伤的，或直接导致较大经济损失的情形。

有下列情形之一的，绩效评价结果认定不合格：

涉及被上级部门或网信部门通报的网络安全事故，以及上级部门或公安部门通报的安全责任事故，认定为发生安全事故。

4.4 结果运用

资金支付管理。季度评价结果与运维费用支付挂钩，根据绩效评价结果，按照合同约定完成运维费进度预支付审核。

合同另有约定的，按照合同执行。

4.5 绩效评价打分表（参照表）

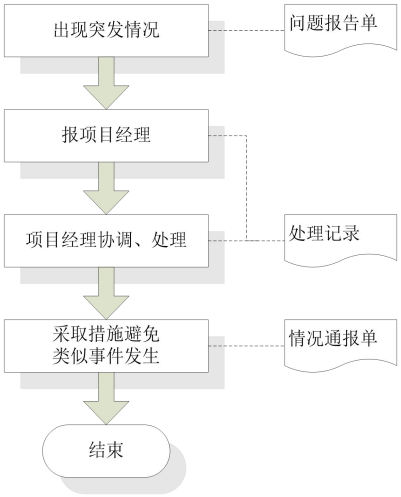
项目类别		评分标准	评价周期	分值		扣分说明	得分		扣分理由
服务交付	周报告计划提价	每周一提交《本周运维服务总结报告》（需包含设备运行分析、故障统计、整改措施）及《次周运维服务计划说明》（需包含人员值班清单、运维计划）提交情况。	周	10	35	迟交扣 1 分，内容不全扣 0.5 分			
	巡检计划落地性	每月对照各模块运维计划和方案，核查巡检记录巡检完成率达 100%，随机选取巡查点位进行现场复核	月	5		未按计划完成巡检，每项扣 1 分；巡检记录与现场情况不符，每处扣 2 分。			
	系统可用性	全年软件因故障中断时间不超过 43.8 小时，硬件设备全年在线率≥95%	月	5		软件不满足可用性要求扣 2 分； 硬件不满足在线率要求扣 2 分；			
	电子留档制度	每月检查运维单位电子档案的完整性、准确性、规范性（所有需留档内容无缺失，覆盖运维全流程；电子档案数据与实际一致；档案格式统一）。台账记录完整度≥90%	月	5		留档内容存在缺失，每缺一项扣 1 分；电子档案数据与实际不一致，每处扣 1 分；电子档案格式不统一，扣 0.5 分。			
	人员值班驻场	根据运维单位每周提交《人员值班清单》抽查核对运维人员驻场值班情况	月	10		未按规定到岗的，每人次扣 1 分；值班记录缺失或信息不全，每处扣 0.5 分			
服务质量	问题整改闭环	巡检发现问题后，形成检查整改台账，明确整改措施和完成时间	周	5	20	问题未按时整改且无正当理由的，每项扣 0.5 分；整改后仍存在同类问题，每重复 1 次扣 0.5 分			
	知识库管理制度	是否建立知识库管理制度；核查运维知识库每月更新情况，随机抽取典型故障案例，检查案例描述（含故障原因、处理步骤、预防措施）的完整性	月	10		未按月更新知识库的，扣 1 分；案例记录额缺项的，每个案例扣 0.5 分。			
	人员配置及保密	核查运维单位提交的《人员配置清单》，对照合同约定岗位（如硬件工程师、安全运维工程师、数据库管理员等），检查岗位覆盖率，汛期人员变动率≤5%。是否建立完善的保密制度，并定期开展人员保密培训。	季	5		岗位缺失的，每个岗位扣 2 分；未定期开展人员保密培训扣 2 分。			
资源管理	运维机构管理制度	是否建立完善的运维机构管理制度，人员配备、单位管理、考勤、考核等内部管理措施是否完善。	季	5	25	制度不健全的，每缺一项扣 1 分。			
	人员资质及安全	运维人员具备相应资质（知识、技能、经验），每季度全覆盖核查 1	季	10		人员资质不符，每人次扣 1 分；因个人操作不规范，			

		次；保证运维人员野外作业合规、安全。				发生事故，每次扣 2 分。			
	备品备件及预算执行管理制度	是否建立备品备件采购、管理制度；是否具有备品备件出入库台账并填写清晰、数量清楚、账实相符，备品库存周转率≥80%； 预算执行偏差率≤5%； 更换设备设施是否符合国家标准；现场抽查出入库记录（需包含领用日期、用途、领用人签字），核对记录与实际库存一致性。	季	10		关键备件库存不足的、入出库记录缺失或与库存不符的，酌情扣分。（制度不健全的，扣 2 分；出入库台账不清晰的，扣 1 分；库存不足的，扣 2 分；更换的设备设施不符合国家标准的，每件扣 1 分；出入库记录与实际库存不一致的，每处扣 1 分。预算执行偏差过大的，扣 2 分。）			
风险管理	电子留档制度	每月检查运维单位电子档案的完整性、准确性、规范性（所有需留档内容无缺失，覆盖运维全流程；电子档案数据与实际一直；档案格式统一）。台账记录完整度≥90%	月	10	20	留档内容存在缺失，每缺一项扣 1 分；电子档案数据与实际不一致，每处扣 1 分； 电子档案格式不统一，扣 0.5 分。			
	数据治理制度、网络安全管理制度	是否建立数据治理制度、网络安全管理制度；抽查数据库备份情况，进行备份恢复测试（随机抽取 1 份核心数据备份进行恢复，验证时长与完整性）；漏洞扫描抽查，检查系统是否存在安全漏洞。	季	10		数据备份恢复不完整，每处关键数据扣 1 分； 数据备份恢复不及时，扣 1 分； 漏洞扫描抽查出现安全漏洞，每处漏洞扣 2 分。			
总计（100 分）									

五、应急保障

虽然已经针对本项目制定了详尽的设计、应急处理预案，整个流程严谨而有序。但是，在服务维护过程中，意外情况将难以完全避免。将对项目实施的突发风险进行详细分析，并且针对各类突发事件，设计了相应的预防与解决措施，同时提供了完整的应急处理流程。

5.1 应急基本流程



5.2 预防措施

针对可能遇到的各种各样的风险，总结多年维护服务经验，针对一些可能出现的情况，制定了一系列预防处理措施，举例如下：

类型	事件	预防措施	处理

类型	事件	预防措施	处理
应用软件	无法启动软件可执行文件	提前准备好各类需维护软件安装程序	将应用软件数据文件备份后，重新安装
	软件打开过程中或运行中异常错误关闭	准备好安装程序，操作系统优化和修补软件，查杀病毒软件	判断出错原因，备份数据，采取相关修复措施
操作系统	使用者本机操作系统异常或系统资源占用严重	准备好系统检查程序及修补程序，以及查杀病毒软件	告知使用者错误原因可能类型，提出解决方案，经使用者认可后采取相应措施
	B/S 结构系统，IE 浏览器异常或无法下载控件	准备流氓软件清理程序、修复浏览器软件、查杀病毒软件	检查 IE 浏览器选项设置，分析原因进行修复

5.3 突发事件应急策略

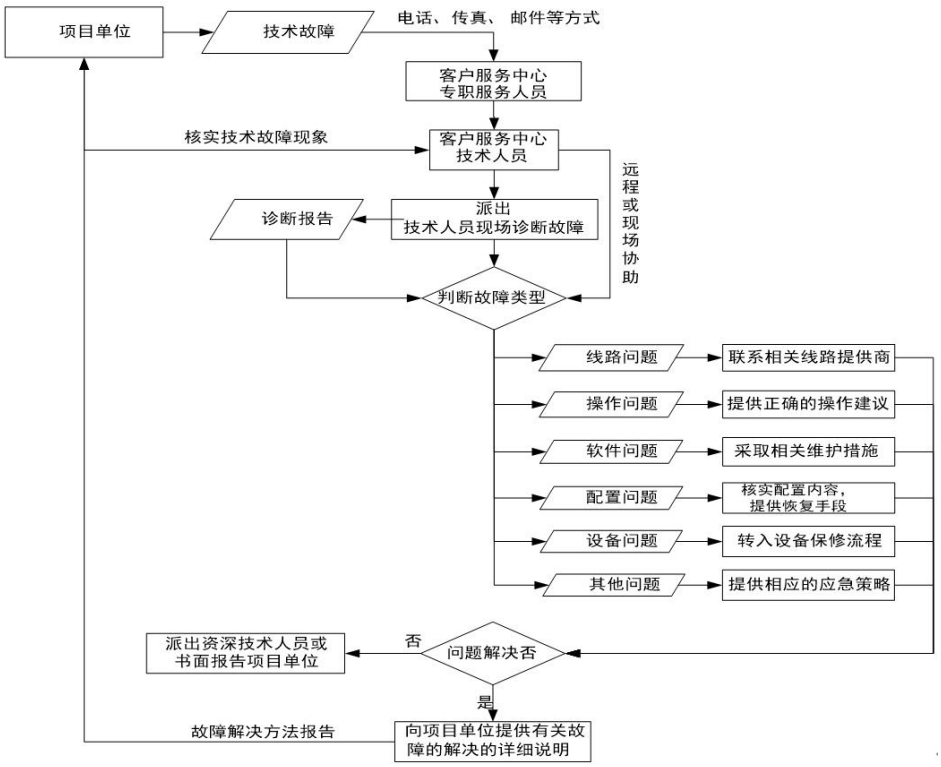
系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，设计了完善的突发事件应急策略。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

对发现的问题在报负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

紧急情况	预防措施	应急策略
硬件损坏	项目单位硬件损坏	在磁盘数据未丢失情况下，保证数据安全性，建议项目单位替换相关硬件。
操作失误	加强培训力度，掌握培训效果，检验操作人员操作水准，提示注意事项。	操作失误未造成即成结果或数据未丢失情况下，保障数据安全，反之，协调相关部门，进行补救。对操作人员强调注意事项
配置丢失	培训时强调使用前配置方法和步骤，并特别提示需在使用前按要求操作	派出上门维护、培训人员重新配置，并耐心讲解。
数据丢失	培训时强调使用过程中注意定期备份重要数据，日常维护过程中，上门服务人员实时备份数据并告知用户	协调有关部门，进行补救，无法补救，提交报告说明原因。

突发事件应急策略服务流程图如下：



5.4 运维质量保障

服务团队需要建立、实施质量管理体系和运行机制来推动服务团队工作的完善和深化，逐步建立起适应本项目需求的服务新体系，使整个项目运行向专业化、科学化、规范化的方向发展。所以需要签订 SLA 服务协议，以保证服务质量和服务效率，并且持续性改进。

服务团队质量管理制度建立后，为进一步加大质量管理力度，增强一线维护人员质量管理意识，QA 主管需根据项目组成员的工作特征，将质量管理进一步细化，有针对性地将质量管理工作进行分工并责任落实到人，力求通过项目组成员的共同努力，达到服务团队质量管理的全面提升。

六、商务要求：

（一）服务期限：

采购包 1（智慧水务及水库监测模块）：各模块运行维护周期

序号	模块名称	运维周期
1	智慧防汛前端监测感知与系统应用开发集成运维模块	7.5 个月
2	西安市水库监测设施模块	12.5 个月
3	西安市水务局智慧水务平台运维模块	7.5 个月

采购包 2（网络安全服务）：自合同签订之日起 1 年。

（二）款项结算：

采购包 1：预付款，合同签订后，达到付款条件起 10 个工作日内，支付合同总金额的 60.0%；

进度款，2027 年主汛期前绩效评价符合条件后，达到付款条件起 10 个工作日内，支付合同总金额的 20.0%；

进度款，项目履约验收完成后，达到付款条件起 10 个工作日内，支付合同总金额的 20.0%；

采购包 2：预付款，合同签订后，达到付款条件起 10 个工作日内，支付合同总金额的 60.0%；

进度款，2027 年主汛期前绩效评价符合条件后，达到付款条件起 10 个工作日内，支付合同总金额的 20.0%；

进度款，项目履约验收完成后，达到付款条件起 10 个工作日内，支付合同总金额的 20.0%；

七、服务清单

7.1 软件运维服务清单

服务类型	服务内容	服务描述	运维对象
日常监控巡检	系统运行状态检查	访问软件平台主界面，验证核心功能页面可正常加载，依次检查各业务模块功能可用性	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	日志与告警信息检查	登录系统日志管理平台，查看当日系统日志，检查告警列表，对异常告警进行初步分析、处理	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	服务器性能监控	检查服务器 CPU、内存、磁盘使用率，监控网络连通性与带宽占用情况，检查应用服务响应时间、处理异常情况	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	数据链路检查	检查数据接收接口是否正常获取外部数据，验证模型推演计算任务的执行状态，确认结果输出接口数据是否及时准确	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
例行维护	系统健康检查	全面检查软件运行健康状态，覆盖系统运行、服务调用、数据交互、性能负载，记录检查结果，每月开展一次。	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	软件补丁升级与版本更新	制定升级计划，明确升级时间窗口，在测试环境验证补丁/版本的兼容性，执行升级操作，按需开展。	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块

			西安市水务局智慧水务平台运维模块
	性能调优	分析系统性能监控数据，定位性能瓶颈，优化配置参数、数据库索引、缓存策略，验证调优效果，按需开展。	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	数据库日常维护	执行数据库碎片整理,检查索引有效性并重建失效索引，更新统计信息，清理历史数据释放存储空间，每月开展一次。	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	系统日志归集与分析	导出系统日志，对日志进行分类归档,分析日志中的异常模式,形成日志分析报告，每月开展一次。	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
数据运维	数据对接与同步	检查内外部数据源连接状态,执行数据同步任务，监控同步进度与结果，处理数据同步失败或异常情况	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	数据备份	制定数据备份计划,明确备份频率与保留策略，执行全量备份与增量备份，定期检查备份文件的完整性	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	数据恢复测试	制定数据恢复测试计划,在测试环境中执行数据恢复操作,验证恢复后数据的完整性与可用性	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	数据操作管理	接收并审核数据添加、修改、删除、导出需求,按规范执行数据操作并记录操作内容与时间,定期审计数据操作记录	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块

	数据治理	围绕数据采集、传输、存储、处理、应用、销毁等全生命周期开展治理活动，确保数据质量符合业务要求	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	模型数据率定及校验	每日检查专业模型的自动运行状态，验证模型输入数据的完整性与及时性，确认模型输出结果的正常生成；	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
响应式维护	需求接收与评估	接收用户系统配置变更、权限调整、业务流程优化需求，评估需求的技术可行性与工作量，制定维护方案并明确实施计划	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	变更实施	在测试环境验证变更方案，在生产环境执行变更操作，验证变更效果确保业务正常运行	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	问题修复与功能完善	收集用户反馈的问题与改进建议，定位问题根因并制定修复方案，实施代码修复或算法升级，进行功能测试与回归测试	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	维护记录留存	记录维护过程（包括操作步骤、变更内容、测试结果），保存操作日志、现场截图等资料，归档维护文档确保可追溯	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
故障处置	故障响应与初步研判	接收故障报告确认故障级别，30 分钟内响应，60 分钟内完成初步研判，判断故障性质并确定处置方案	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	现场处置	接到通知后 1 小时内抵达现场，现场排查故障根因，执行应急恢复措施	智慧防汛前端监测感知与系统应用开发集成运维模块

			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	故障定位与修复	一般故障 2 小时内完成排查与修复，重大故障 6 小时内完成全面处置，验证修复效果确认系统功能恢复正常	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	故障分析与总结	分析故障根因形成故障分析报告，制定标准化解决方案与预防措施，更新故障知识库	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	故障闭环	输出事件处理文档，确认用户满意度，归档故障处置资料	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
技术支持与服务	服务响应	7×24 小时接听服务热线，记录用户问题描述与需求，根据问题类型分配技术人员	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	远程技术支撑	通过远程工具诊断系统问题，指导用户进行问题排查，无法远程解决时安排现场支持	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	专业技术支撑	为用户提供系统应用咨询，解读预报结果提供数据分析服务，协助用户制定业务解决方案	智慧防汛前端监测感知与系统应用开发集成运维模块
			西安市水库监测设施模块
			西安市水务局智慧水务平台运维模块
	基础操作指导	指导用户进行系统基础操作，解答常见问题（FAQ），协助用户进行数据调用	全部

	培训服务	制定培训计划与培训材料，开展系统操作培训和业务应用培训，评估培训效果	全部

7.2 硬件运维服务清单

服务类型	服务内容	服务描述	运维对象	设备数量
日常监控巡检	在线状态监控	（1）执行设备在线状态核查：非汛期每日 1 次核查设备在线情况，汛期每日 2 次。 （2）检查所有前端感知设备、视频监控设备、网络设备在线状态。 （3）记录设备在线率、离线设备信息及原因分析。 （4）对离线设备进行标记并通知相关运维人员。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
	现场巡检	（1）前端监测站点、视频监控、网络通信、供电配套设备，每季度 1 次现场巡检。 （2）服务器、存储设备：每月 1 次现场维护。 （3）到达现场后，逐一检查设备物理状态、运行指示灯、连接线路。 （4）执行设备清洁、紧固、调试等现场维护操作。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
	专项巡检	（1）定期核查网络设备系统版本与安全规则配置。 （2）检查视频监控画面清晰度、流畅度及录像回放功能。 （3）汛期对防汛关键硬件开展专项高频巡检。 （4）形成专项巡检报告，记录发现的问题及整改建议。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
例行维护	设备清洁保养	（1）每季度对所有设施设备进行灰尘清洁。 （2）擦拭摄像头镜头与外壳，确保画面清晰。 （3）加固摄像头支架，检查固定螺栓紧固情况。 （4）调试视频监控点位角度与焦距，确保监控范围合适。 （5）清洁机箱内部灰尘，检查风扇运转情况。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
	硬件性能优化	（1）测试校准电源稳压器输出电压，确保电压稳定在额定范围。 （2）优化防火墙规则，删除无效规则，优化规则匹配顺序。 （3）优化路由策略，调整路由表，减少不必要的路由跳转。 （4）优化安全策略，关闭风险端口，限制不必要的服务。 （5）提升服务器、存储设备 IO 性能，优化磁盘读写策略。 （6）测试网络响应时间，确保符合业务要求。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
	系统固件维护	（1）完成服务器等设备的系统安全加固。 （2）优化服务器内核参数，提升系统性能。 （3）安装系统安全补丁与功能更新。 （4）升级网络设备、网关、路由器安全补丁与系统版本。 （5）定期备份网络设备配置文件。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52

		（6）验证升级后设备功能正常，无兼容性问题。	防火墙	15
	预防性维护	（1）定期检查设备老化情况，制定部件更换计划。 （2）更换老化、有故障风险的硬件部件（如硬盘、风扇、电源等）。 （3）排查硬件隐患，检查设备运行异常记录。 （4）预防性更换即将过期的配件（如电池、线缆等）。 （5）记录预防性维护情况，形成维护台账。	视频监控	163
			服务器	5
			交换机	25
			硬盘录像机	9
			路由器	1
			网关	52
			防火墙	15
响应式维护	配置与参数调整	（1）接收业务部门硬件配置变更需求。 （2）评估变更需求的可行性与影响范围。 （3）在测试环境验证配置变更方案。 （4）在生产环境执行硬件配置变更。 （5）更新设备信息登记，调整监控参数阈值。 （6）验证变更效果，确保设备正常运行。	全部	294
	策略与证书管理	（1）评估现有网络策略的合理性。 （2）根据业务需求优化网络策略、安全策略。 （3）检查 SSL/TLS 证书有效期，提前 30 天预警。 （4）更新即将到期的 SSL/TLS 证书。 （5）验证新证书部署生效，无访问异常。 （6）完善安全策略，封堵新增的安全风险点。	全部	294
故障处置	故障处置服务	（1）接收硬件设备故障报告，确认故障等级。 （2）30 分钟内响应，开始初步故障诊断。 （3）汛期 3 小时内、非汛期 6 小时内人员到达现场（城区）。 （4）现场排查故障原因，制定处置方案。 （5）执行故障修复操作。 （6）汛期 8 小时内、非汛期 24 小时内完成故障排除。 （7）验证设备恢复正常运行。	全部	294
	记录与闭环	（1）详细记录故障发生时间、设备名称、型号。 （2）记录故障现象及用户描述。 （3）记录排查过程、诊断结果及处理措施。 （4）记录故障修复结果及验证情况。 （5）形成故障处置闭环文档。 （6）更新故障知识库。	全部	294
	故障汇总分析	（1）每月汇总所有硬件故障记录。 （2）分析故障类型分布（设备类型、故障原因）。 （3）定位频发问题，识别高故障率设备或部件。 （4）分析故障原因，找出根本原因。 （5）制定预防性措施和改进方案。 （6）更新预防性维护计划。	全部	294

7.3 备品备件清单

序号	名称	型号	数量	备注
1	监控摄像头	X6741-20-G240-E2-Wp	2	双目镜头（变焦镜头，定焦镜头）
2	融合网关	WDHV-01	2	
3	无线路由器	无线路由器	4	

4	视频工业级 4G 路由器		10	

7.4 硬件设备台账

设备类型	设备型号	数量	建设时间	验收时间	质保周期	安装位置	设备现状	备注
城市积水点视频监控	DS-2DE44ZFIW-DZ、	48 套	2025 年	2025 年 12 月	2025 年 12 月 9 日到 2027 年 12 月 9 日	积水点	正常	
	YXP-275W、YXBTL-12.8V(200AH)、YXC-HC2440、YXSD-275W-1、YXBX-3	27 套	2025 年	2025 年 12 月	2025 年 12 月 9 日到 2027 年 12 月 9 日	积水点	正常	
排口视频监控	iDS-2DF7C425IXR-A(T5)(B)、YXP-275W、YXBTL-12.8V(200AH)、YXC-HC2440、YXSD-275W-1、YXBX-3	36 套	2025 年	2025 年 12 月	2025 年 12 月 9 日到 2027 年 12 月 9 日	排水口	正常	
河道视频监控	DS-2DF7C425IXR-A(T5)(B)、YXP-275W、YXVRLA-N-12200、YXC-HC2440、YXSD-300W-2、YXBX-3	35 套	2025 年	2025 年 12 月	2025 年 12 月 9 日到 2027 年 12 月 9 日	河道	正常	
计算服务器	百信恒山 326RA	2 台	2025 年	2025 年 12 月	2025 年 12 月 9 日至 2028 日 12 月 9 日	凤八机房	正常	属于市水务局的维护
渲染节点服务器	宏碁/acer、Veriton H500	3 台	2025 年	2025 年 12 月	2025 年 12 月 9 日到 2027 年 12 月 9 日	水务局	正常	属于市水务局的维护
交换机	华为 S5720S-52P-LI-AC	1 台	2021	2023 年 6 月 29 日	2023 年 6 月 29 日至 2025 年 6 月 29 日	防汛仓库	正常	
枪球一体摄像机	杭州海康威视数字技术股份有限公司 iDS-2SE7C124MW-D(23X/F1)(S5)(B)	18 台	2021	2023 年 6 月 29 日	2023 年 6 月 29 日至 2025 年 6 月 29 日	防汛仓库	正常	
NVR 硬盘录像机	杭州海康威视数字技术股份有限公司	1 台	2021	2023 年 6 月 29 日	2023 年 6 月 29 日至 2025 年 6 月 29 日	防汛仓库	正常	

	DS-8664NX-I8							
光纤交换机	广州光桥通信设备有限公司 光桥 GQ-IES204G	20 台	2021	2023 年 6 月 29 日	2023 年 6 月 29 日至 2025 年 6 月 29 日	防汛仓库	正常	
路由器	华为 S5720S-52P-LI-AC	1 台	2021	2023 年 6 月 29 日	2023 年 6 月 29 日至 2025 年 6 月 29 日	防汛仓库	正常	
边缘融合数据网关	MCU-16G（WDHV-01）	42 套	2022 年	2026 年 1 月 15 日	区县基础设施、视频监控、视频会议、物联网平台出厂后质保 3 年，2022 年 12 月上述设备进场报验完成，截止 2025 年 12 月质保均已到期	水库	正常	
监测站出口防火墙	USG6510E	10 套	2022 年	2026 年 1 月 15 日		水库	正常	
视频一体杆（球形摄像机、支持 4G 传输、立杆、防雷、供电）	X6741-20-GZ40-E2-Wp	16 套	2022 年	2026 年 1 月 15 日		水库	正常	
万兆接入交换机	FutureMatrix S6735-S24X6C	4 台	2022 年	2026 年 1 月 15 日		水库	正常	
监测数据管理存储设施	PR210K32	8 台	2022 年	2026 年 1 月 15 日		水库	正常	
网络硬盘录像机(工业级）	MV3500-04	8 台	2022 年	2026 年 1 月 15 日		水库	正常	
区县出口防火墙	USG6525E-AC	4 台	2022 年	2026 年 1 月 15 日		水库	正常	
边缘融合数据网关	南京岩思工程仪器、 MCU-16-DN-G	10 套	2023 年	2025 年 10 月 13 日	2025 年 10 月 13 日至 2026 年 10 月 13 日	水库	正常	
监测站出口防火墙	华为技术有限公司 USG6311E-AC	1 套	2023 年		025 年 10 月 13 日至 2026 年 10 月 13 日	水库	正常	
视频一体杆（球形摄像机、支持 4G 传输、立杆、防雷、供电）	华为技术有限公司 X6741-20-GZ40-E2-Wp	10 套	2023 年		025 年 10 月 13 日至 2026 年 10 月 13 日	水库	正常	

八、其他技术要求：

（1）维护软件所支出的费用以及各应用系统日常问题处理支出(主要包括软件日常维护、数据维护、安全维护以及现有功能的优化完善),包含定制软件系统和通用软件(如存储系统、操作系统、中间件等)。

（2）安全运维服务:对保障信息系统安全相关的安全产品(包含数据库安全审计、防火墙、安全网关、态势感知、应用防护、检测管理等)续保费用,软硬件实施例行操作、响应支持、调研评估和优化改善等服务,如监测预警及应急响应、防护加固。

（3）系统迁移上云：按照甲方要求，完成相关信息系统迁移上云。

（4）物联网平台设备迁移：按照甲方要求，完成相关物联网前端感知设备迁移至大数据中心物联网平台，完成存量监控设备迁移至甲方指定的视频平台。

（5）如受政策影响造成资金支付进度延迟，双方协商解决。

（6）安全运维是一个整体，需要各方共同配合完成：模块运维单位（包 1）为系统安全负主体责任，负责整体系统的安全运行并完成整改及漏洞修复以及模块功能优化升级等工作，重要保障时期和上级攻防演练期间，提前做好应对，安排专人驻场，落实防范措施，确保安全。

测评机构及评估单位（包 2）作为检查测评主体，负责落实安全评估等安全工作。各单位协同做好安全工作，若有未落实责任情形导致系统出现安全事件，追究相应责任，根据绩效评价扣除相应费用。重要保障时期和上级攻防演练期间，提前做好应对，安排专人驻场，落实防范措施，确保安全。